CLAIMS

What is claimed is:

1. A method to verify configuration of a client access device requesting access to a network, the method including:

establishing a communications link with the client access device to authenticate and authorize a user associated with the client access device;

receiving client device configuration data from the client access device over the communications link during an authentication and authorization exchange;

processing the client device configuration data; and

selectively granting the client access device access to the network based upon the client device configuration data.

2. The method of claim 1, wherein processing the client device configuration data includes determining if the client device configuration data meets predetermined security requirements.

3. The method of claim 2, wherein determining if the client device configuration data meets predetermined security requirements includes comparing the client device configuration data with reference configuration data.

4. The method of claim 2, which includes updating the client device configuration data if the client device configuration data fails to meet the predetermined security requirements.

5. The method of claim 4, wherein selectively granting the client access device access to the network includes, denying access to the network if the client device configuration data is not updated.

6. The method of claim 1, wherein the establishing of the communications link with the client access device includes, communicating an agent to the client access device, the agent operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network.

7. The method of claim 6, which includes, if after the processing of the client device configuration data the client device configuration data requires an update, using the agent to update the client access device with updated configuration data.

8. The method of claim 7, which includes, after updating the client access device, receiving an update result indicator from the agent to confirm that the configuration of the client access device has been updated.

9. The method of claim 1, wherein the establishing of the communications link with the client access device includes communicating a command set, which includes at least one command, to the client access device, the command set operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network.

10. The method of claim 9, which includes, if after the processing of the client device configuration data the client device configuration data requires an update, using the command set to update the client access device with updated configuration data.

11. The method of claim 10, wherein the command set further includes a first command set to identify and communicate the client device configuration data to the server, and a second command set to update the client access device with the updated configuration data.

12. The method of claim 10, which includes, after updating the client access device, receiving an update result indicator from the client access device to confirm that the configuration of the client access device has been updated.

13. The method of claim 1, which includes, after establishing communications with the client access device, authenticating a user associated with the client access device.

14. The method of claim 13, wherein authenticating the user includes verifying user login information associated with the user attempting access to the network.

15. The method of claim 1, wherein the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data.

16. A system to verify configuration data of a client access device requesting access to a network, the system including:

a network access server, coupled to a network, to establish a communications link to the client access device to authenticate and authorize a user associated with the client access device and to receive the client device configuration data from the client access device over the communications link during an authentication and authorization exchange; and

at least one further server coupled to the network access server to process received configuration data and to selectively grant the client access device access to the network based upon the received client device configuration data.

17. The system of claim 16, wherein the at least one further server includes a configuration server to process the client device configuration data such that the configuration server determines if the client device configuration data meets predetermined security requirements.

18. The system of claim 17, wherein the configuration server compares the client device configuration data with reference configuration data to determine if the client device configuration data meets predetermined security requirements.

19. The system of claim 17, wherein the configuration server, after the client device configuration data is processed, updates the client device configuration data.

20. The system of claim 19, wherein the configuration server denies network access to the client access device if the client device configuration data is not updated.

21. The system of claim 17, wherein to establish the communications link with the client access device, the network access server communicates an agent to the client access device, the agent operable to identify the client device configuration data and to communicate the client device configuration data to at least one of the network access server and the configuration server.

22. The system of claim 21, wherein if after the processing of the client device configuration data the client device configuration data requires an update, the

configuration server being configurable to use the agent to update client device configuration data with updated configuration data.

23. The system of claim 22, wherein after the agent updates the client access device, the configuration server receives an update result indicator from the agent to confirm that the configuration of the client device has been updated.

24. The system of claim 17, wherein to establish the communications link with the client access device, the network access server communicates a command set to the client access device, the command set operable to identify the client device configuration data and to communicate the client device configuration data to at least one of the network access server and the configuration server.

25. The system of claim 24, wherein if after the processing of the client device configuration data, the client device configuration data requires an update, the configuration server is operable to further use the command set to update client device configuration data with updated configuration data.

26. The system of claim 25, wherein after the configuration server updates the client access device, the configuration server receives an update result indicatior from the client access device to confirm that the client configuration has been updated.

27. The system of claim 24, wherein the command set further includes a first command set to identify and communicate the client device configuration data to the server, and a second command set to update the client access device with the updated configuration data.

28. The system of claim 16, wherein the at least one further server includes an authentication server to authenticate and authorize a user associated with the client access device.

29. The system of claim 16, wherein the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data.

30. A machine readable medium storing a set of instructions that, when executed by a machine, cause the machine to:

establish a communications link with a client access device to authenticate and authorize a user associated with the client access device;

receive client device configuration data from the client access device over the communications link during an authentication and authorization exchange;

process the client device configuration data; and

selectively grant the client access device access to the network based upon the client device configuration data.

31. The machine readable medium of claim 30, wherein after the processing of the client device configuration data, the client device configuration data is updated with updated configuration data.

32. A method to manage access to a network from a client access device, the method including:

requesting access to the network;

authenticating a user associated with the client access device in an authentication and authorization exchange;

communicating client device configuration data to a network access system;

receiving a verification response from the network access system; and

accessing the network if the user is authenticated and the verification response from the network access system accepts the client device configuration data.

33. The method of claim 32, wherein prior to receiving a verification response, updated configuration data is received from the network access system to replace the client device configuration data.

34. A machine readable medium storing a set of instructions that, when executed by a machine, cause the machine to:

request access to a network;

authenticate and authorize a user associated with the client access device in an authentication and authorization exchange;

communicate client device configuration data to a network access system during the authentication and authorization exchange;

receive a verification response from the network access system; and

access the network if the user is authenticated and the verification response from the network access system accepts the client device configuration data.

35. The machine readable medium of claim 34, wherein prior to receiving a verification response, updated configuration data is received from the network access system during the authentication and authorization exchange to replace the client device configuration data.

36. A method of controlling access by a client device to a network in a multi-party service access environment, the method including:

receiving an access request from the client device to access the network in an authentication and authorization exchange;

receiving configuration data from the client device during the authentication and authorization exchange, the configuration data identifying a security status of the client device; and

selectively granting the client device access to the network based on the configuration data.